STATE OF WEST VIRGINIA
OFFICE OF THE ATTORNEY GENERAL
DARRELL V. MCGRAW, JR.
CONSUMER PROTECTION DIVISION
1-800-368-8808 or 304-558-8986

Press Release

FOR IMMEDIATE RELEASE

November 24, 2009

Contact: Jill L. Miles
Phone: (800) 368-8808

Scamsters Attempt to Hook the West Virginia Attorney General's Office with Phishing Scam

Last week, the West Virginia Attorney General's Office received the following email:

> Dear customer
>
> We regret to inform you that you Bank of America Online Account has been temporarily suspended. Your account has been suspended after too many failed login attempts have been made. This is most likely an attempt to gain unauthorized access to your account and/or personal information.
>
> To resolve this problem we have attached a form to this email. Please download the form open it and follow the instructions on your screen.
>
> Bank of America, Member FDIC
> 2009 Bank of America Corporation. All Rights Reserved.

Attached to the email was a form which instructed the recipient to provide a wide range of personal information, including their date of birth, Social Security number, mother's maiden name, and credit card number.

West Virginians are receiving similar emails on a daily basis and Attorney General McGraw wants to warn them not to respond. "It's a scam called "phishing" – and it involves Internet fraudsters who send spam or pop-up messages to lure personal information (credit card numbers, bank account information, Social Security number, passwords, or other sensitive information) from unsuspecting victims," explained McGraw.

Phishers send an email or pop-up message that claims to be from a business organization that you may deal with – for example, an Internet service provider (ISP), bank, online payment service, or even a government agency. The message will ask you to "update," "validate," or "confirm" your account information. The messages direct you to a website that looks just like a legitimate organization's site. But it isn't. It's a bogus site whose sole purpose is to trick you into divulging your personal information so the operators can steal your identity and run up bills or commit crimes in your name.

The West Virginia Attorney General's Office suggests the following tips to help you avoid getting hooked by a phishing scam:

• If you get an email or pop-up message that asks for personal or financial information, do not reply and don't click on the link

in the message, either. Legitimate companies don’t ask for this information via email. If you are concerned about your account, contact the organization mentioned in the email using a telephone number you know to be genuine, or open a new Internet browser session and type in the company’s correct Web address yourself.

• Area codes can mislead. Some scammers send an email that appears to be from a legitimate business and ask you to call a phone number to update your account or access a "refund." Because they use Voice Over Internet Protocol technology, the area code you call does not reflect where the scammers really are.

• Use anti-virus and anti-spyware software, as well as a firewall, and update them all regularly. Anti-virus software and a firewall can protect you from inadvertently accepting such unwanted files. Anti-virus software scans incoming communications for troublesome files. Look for anti-virus software that recognizes current viruses as well as older ones; that can effectively reverse the damage, and that updates automatically.

A firewall helps make you invisible on the Internet and blocks all communications from authorized sources.

• Don’t email personal or financial information. Email is not a secure method of transmitting personal information. If you initiate a transaction and want to provide your personal or financial information through an organization’s website, look for indicators that the site is secure, like a lock icon on the browser’s status bar or a URL for a website that begins "https:’ (the "s" stands for "secure").

• Review credit card and bank account statements as soon as you receive them to check for unauthorized charges. If your statement is late by more than a couple of days, call your credit card company or bank to confirm your billing address and account balances.

• Be cautious about opening any attachment or downloading any files from email you receive.

• Forward spam that is phishing for information to spam@uce.gov and to the company, bank, or organization impersonated in the phishing email.

If you believe you’ve been scammed, file a complaint with the West Virginia Attorney General’s Office at www.wvago.gov or by calling its toll-free number at 1-800-368-8000.

##